

FILEDUNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO**United States District Court** MAY 03 2016

DISTRICT OF NEW MEXICO

MATTHEW J. DYKMAN
CLERK

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

The premises known as: 77 Somerset Drive SE,
Rio Rancho, New Mexico 87124, including all storage
areas and trash containers; and the person of Russell
Romero**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

CASE NUMBER:

16mr346

I, Rhonda Bowie being duly sworn depose and say:I am a(n) United States Postal Inspector and have reason to believe

Official Title

that ☐ on the person of or ☒ on the premises known as (name, description and/or location)**See Attachment "A" incorporated by reference herein**in the _____ District of New Mexico

there is now concealed a certain person or property, namely (describe the person or property)

See Attachment "B" incorporated by reference herein

which is (give alleged grounds for search and seizure under Rule 41(b) of the Federal Rules of Criminal Procedure):

Property that constitutes evidence of the commission of a criminal offense; or
Contraband, the fruits of crime, or things otherwise criminally possessed; or
Property designed or intended for use or which is or has been used as the means of committing a criminal offense;in violation of Title 18 United States Code, Section(s) 2252(a)(1), 2252A(a)(1),
Title 18 United States Code, Section(s) 2252(a)(4)(B), 2252A(a)(5)(B) and Title 18 United States Code, Section(s)
2252(a)(2), 2252A(a)(2). The facts to support the issuance of a Search Warrant are as follows:**See attached Affidavit incorporated by reference herein.**Rhonda Bowie
Signature of Affiant

Sworn to before me, and subscribed in my presence

May 3, 2016
Dateat Albuquerque, New Mexico
City and StateSteven C. Yarbrough
Name and Title of Judicial OfficerU.S. Magistrate JudgeSteven C. Yarbrough
Signature of Judicial Officer

DAMON P. MARTINEZ
United States Attorney
Jonathon Gerson
Assistant United States Attorney
201 3RD St. NW, Suite 900
Albuquerque, NM 87102
(505) 346-7274

United States District Court District of New Mexico

IN THE MATTER OF THE SEARCH OF THE
PREMISES KNOWN AS: 77 Sommerset Drive
SE, Rio Rancho, New Mexico 87124, including all
storage areas and trash containers; and the person
of Russell Romero

Mag No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Rhonda Bowie, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant to search the entire premises of 77 Sommerset Drive SE, Rio Rancho, New Mexico 87124-3374. Listed and described in Attachment A, for the items specified in Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service (USPIS), assigned to the Phoenix Division, in Phoenix, AZ. I have been so employed since 1995. As a United States Postal Inspector, I am responsible for the investigation of Federal offenses involving the transportation, distribution, receipt, and sale of material depicting the Sexual Exploitation of Children. From September of 1995 until June of 2001, I was employed as the Child Exploitation Specialist of the Phoenix Division of the USPIS in Phoenix, Arizona. From November of 2003 until April of 2005, I was assigned as one of the Child Exploitation Specialists of the Los Angeles Division of the USPIS in

1 Los Angeles, California. From April of 2005 until approximately June of 2008, I was assigned as the
2 Child Exploitation Specialist of the San Francisco Division of the USPIIS in Sacramento, California. I
3 am currently assigned as the Child Exploitation Specialist of the Phoenix Division, in Phoenix,
4 Arizona, and have been so assigned since June of 2014. I have received training in the area of child
5 pornography and child sexual exploitation as well as specialized instruction on how to conduct
6 investigations of child sexual exploitation and child pornography through the USPIIS and the
7 Department of Justice. I have conducted several investigations of individuals suspected of receiving
8 and distributing child pornography and have participated in the execution of numerous search warrants
9 which have resulted in the seizure of multiple items of child pornography.

10 3. The facts set forth in this affidavit are based on my personal observations, my training
11 and experience, and information provided by U.S. Postal Inspectors, the National Center for Missing &
12 Exploited Children, and Twitter Inc. This affidavit is intended to show merely that there is sufficient
13 probable cause for the requested warrant and does not purport to set forth all of my knowledge of the
14 investigation into this matter. Unless specifically indicated otherwise, all conversations and statements
15 described in this affidavit are related in substance and in part only.

16 4. I have probable cause to believe that evidence of the transportation, distribution, and
17 possession of child pornography in violation of 18 U.S.C. § 2252(a)(1), 18 U.S.C. § 2252A(a)(1) and
18 18 U.S.C. § 2252(a)(4)(B), 18 U.S.C. § 2252A(a)(5)(B), and 18 U.S.C. § 2252(a)(2), 18 U.S.C. §
19 2252A(a)(2) is located at 77 Sommerset Drive SE, Rio Rancho, New Mexico 87124. Based on my
20 training and experience and the facts as set forth in this affidavit, there is probable cause to believe that
21 evidence, fruits, and instrumentalities of criminal violations of 18 U.S.C. § 2252(a)(1), 18 U.S.C. §
22 2252A(a)(1) and 18 U.S.C. § 2252(a)(4)(B), 18 U.S.C. § 2252A(a)(5)(B), and 18 U.S.C. § 2252(a)(2),
23 18 U.S.C. § 2252A(a)(2) are present at the location described in Attachment A.

APPLICABLE DEFINITIONS

5. The term “minor,” as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”

6. The term “lascivious exhibition of the genitals or pubic area of any person” many courts have utilized the following list of factors which were set forth in *United States v. Dost*, 636 F. Supp. 828, 832 (S.D. Cal. 1986), *aff d sub nom. United States v. Wiegand*, 812 F. 2d (9th Cir. 1987):

- whether the focal point of the visual depiction is on the child’s genitalia or pubic area;
- whether the setting of the visual depiction sexually suggestive, i.e. in a place or pose generally associated with sexual activity;
- whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child;
- whether the child is fully or partially clothed, or nude;
- whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;
- whether the visual depiction is intended or designed to elicit a sexual response in the viewer.

7. In *Dost*, the court noted that a visual depiction need not involve all these factors to be a “lascivious exhibition of the genitals or pubic area.” *ID.* At 832. The determination will have to be made based on the overall content of the visual depiction, taking into account the age of the minor. *ID.* No single factor should be given undue weight and a depiction need not involve all the factors in order to be lascivious. *ID.*

8. The term “sexually explicit conduct,” as used herein, is defined pursuant to Title 18 § 2256(2)(A) as “actual or simulated-(i) sexual intercourse, including genital-genital, oral-genital, or

1 oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv)
2 sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.”

3 9. The term “visual depiction,” as used herein, is defined pursuant to Title 18, U.S.C. §
4 2256(5) to include “undeveloped film and videotape, data stored on computer disk or by electronic
5 means which is capable of conversion into a visual image.”

6 10. The term “child pornography” as used herein, is defined pursuant to Title 18, U.S.C. §
7 2256(8)(A) to include any photograph, film, video, picture, or computer or computer-generated image
8 or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit
9 conduct, where the production of such visual depiction involves the use of a minor engaging in
10 sexually explicit conduct, and which is of such conduct.

11 11. The term “child erotica” as used herein, means any material relating to minors that
12 serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual
13 aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually
14 explicit.

15 12. The term “computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as
16 “an electronic, magnetic, optical, electrochemical, or other high speed data processing device
17 performing logical or storage functions, and includes any data storage facility or communications
18 facility directly related to or operating in conjunction with such device.”

19 13. The term “computer hardware,” as used herein, consists of all equipment which can
20 receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic,
21 magnetic, or similar computer impulses or data. Computer hardware includes any data-processing
22 devices (including, but not limited to, central processing units, internal and peripheral storage devices
23 such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage
24 devices), peripheral input/output devices (including, but not limited to, keyboards, printers, video

1 display monitors, and related communications devices such as cables and connections), as well as any
2 devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but
3 not limited to, physical keys and locks).

4 14. The term “computer software,” as used herein, is digital information which can be
5 interpreted by a computer and any of its related components to direct the way they work. Computer
6 software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run
7 operating systems, applications, and utilities.

8 15. The term “computer-related documentation,” as used herein, consists of written,
9 recorded, printed, or electronically stored material which explains or illustrates how to configure or use
10 computer hardware, computer software, or other related items.

11 16. The phrase “computer passwords and data security devices,” as used herein, refers to
12 information or items designed to restrict access to or hide computer software, documentation, or data.
13 Data security devices may consist of hardware, software, or other programming code. A password (a
14 string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data
15 security devices. Data security hardware may include encryption devices, chips, and circuit boards.
16 Data security software of digital code may include programming code that creates “test” keys or “hot”
17 keys, which perform certain pre-set security functions when touched. Data security software or code
18 may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable,
19 as well as reverse the process to restore it.

20 17. The term “Electronic Service Providers” (ESPs), as used herein, is defined pursuant to 18
21 U.S.C. § 2510 as an “Electronic Communications Service” which refers to any service which provides
22 to users thereof the ability to send or receive wire or electronic communications.

23 18. The term “Internet Service Providers” (ISPs), as used herein, refers to commercial
24 organizations that are in business to provide individuals and businesses access to the Internet. ISPs

1 provide a range of functions for their customers including access to the Internet, web hosting, e-mail,
2 remote storage, and co-location of computers and other communications equipment. ISPs can offer a
3 range of options in providing access to the Internet including telephone based dial-up, broadband based
4 access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based
5 subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called
6 bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a
7 user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected
8 by the subscriber. By using a computer equipped with a modem, the subscriber can establish
9 communication with an ISP over a telephone line, through a cable system or via satellite, and can
10 access the Internet by using his or her account name and personal password.

11 19. The term “Internet protocol address” or “IP address,” as used herein, refers to a unique
12 number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP
13 assigns a different unique number to a computer every time it accesses the Internet. IP addresses might
14 also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the
15 computer accesses the Internet.

16 20. The term “website,” as used herein, means a related collection of World Wide Web
17 (WWW) files that usually include a beginning file called a homepage, generally located on the same
18 server, and prepared and maintained as a collection of information by a person, group, or organization.
19 A company or an individual will typically tell you how to get to their website by giving you the
20 address of their home page. From the home page, you can typically get to all the other pages on their
21 site, unless they are password protected. For example, the website for Amazon is www.amazon.com/
22 and there are millions of Web pages that make up the site.

23 21. The terms “records,” “documents,” and “materials,” as used herein, include all
24 information recorded in any form, visual or aural, and by any means, whether in handmade form

(including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

22. The National Center for Missing & Exploited Children (NCMEC) as used herein, refers to a private, nonprofit organization which provides services nationwide to families and professionals relating to preventing the abduction and sexual exploitation of children. NCMEC operates the CyberTipline and Child Victim Identification Program to provide assistance to law enforcement and others in their efforts to identify and rescue victims of child pornography and child sexual exploitation. NCMEC also works with electronic service providers and others in their efforts to reduce the distribution of child sexual exploitation images and videos on the Internet.

23. The Electronic Service Provider (ESP) Twitter Inc. (Twitter) as used herein, refers to a company that owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

24. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to

1 identify his or her Twitter account. The Twitter user may also change this username, password, and
2 name without having to open a new Twitter account.

3 25. Twitter asks users to provide basic identity and contact information, either during the
4 registration process or thereafter. This information may include the user's full name, e-mail addresses,
5 physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and
6 other personal identifiers. For each user, Twitter may retain information about the date and time at
7 which the user's profile was created, the date and time at which the account was created, and the
8 Internet Protocol ("IP") address at the time of sign-up. IP address information can help to identify
9 which computers or other devices were used to access a given Twitter account.

10 26. A Twitter user can post a personal photograph or image (also known as an "avatar") to
11 his or her profile, and can also change the profile background or theme for his or her account page. In
12 addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

13 27. Twitter also keeps IP logs for each user. These logs contain information about the
14 user's logins to Twitter including, for each access, the IP address assigned to the user and the date
15 stamp at the time the user accessed his or her profile.

16 28. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of
17 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to
18 Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition,
19 when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that
20 Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the
21 user with a list of other users who have favorited or retweeted the user's own Tweets, as well as a list
22 of all Tweets that include the user's username (*i.e.*, a list of all "mentions" and "replies" for that
23 username).

1 29. Twitter users can include photographs or images in their Tweets. Each Twitter account
2 also is provided a user gallery that includes images that the user has shared on Twitter, including
3 images uploaded by other services.

4 30. Twitter users can also opt to include location data in their Tweets, which will reveal the
5 users' locations at the time they post each Tweet. This "Tweet With Location" function is off by
6 default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past
7 location data.

8 31. When Twitter users want to post a Tweet that includes a link to a website, they can use
9 Twitter's link service, which converts the longer website link into a shortened link that begins with
10 <http://t.co>. This link service measures how many times a link has been clicked.

11 32. A Twitter user can "follow" other Twitter users, which means subscribing to those
12 users' Tweets and site updates. Each user profile page includes a list of the people who are following
13 that user (*i.e.*, the user's "followers" list) and a list of people whom that user follows (*i.e.*, the user's
14 "following" list). Twitter users can "unfollow" users whom they previously followed, and they can
15 also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom
16 they approve, rather than to the public (which is the default setting). A Twitter user can also group
17 other Twitter users into "lists" that display on the right side of the user's home page on Twitter.
18 Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of
19 Twitter accounts that the user may find interesting, based on the types of accounts that the user is
20 already following and who those people follow.

21 33. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to
22 one of his or her followers. These messages are typically visible only to the sender and the recipient,
23 and both the sender and the recipient have the power to delete the message from the inboxes of both
24

1 users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older
2 DMs are stored on Twitter's database.

3 34. Twitter users can configure the settings for their Twitter accounts in numerous ways.
4 For example, a Twitter user can configure his or her Twitter account to send updates to the user's
5 mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent
6 to the user's phone.

7 35. Twitter includes a search function that enables its users to search all public Tweets for
8 keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

9 36. Twitter users can connect their Twitter accounts to third-party websites and
10 applications, which may grant these websites and applications access to the users' public Twitter
11 profiles.

12 37. If a Twitter user does not want to interact with another user on Twitter, the first user can
13 "block" the second user from following his or her account.

14 APPLICABLE STATUTES

15 38. Title 18 U.S.C. § 2252(a)(1), 18 U.S.C. § 2252A(a)(1) makes it a federal criminal
16 offense for any person to knowingly transports or ships using any means or facility of interstate or
17 foreign commerce or in or affecting interstate or foreign commerce by any means including by
18 computer or mails, any child pornography.

19 39. Title 18 U.S.C. § 2252(A)(5)(B), 2252(a)(4)(B) makes it a federal criminal offense for
20 any person to knowingly possess, or knowingly access with intent to view, any book, magazine,
21 periodical, film, videotape, computer disk, or any other material that contains an image of child
22 pornography that has been mailed, or shipped or transported using any means or facility of interstate or
23 foreign commerce or in or affecting interstate or foreign commerce by any means, including by
24 computer, or that was produced using materials that have been mailed, or shipped or transported using

1 any means or facility of interstate or foreign commerce or in or affecting interstate or foreign
2 commerce by any means, including by computer.

3 40. Title 18 U.S.C. § 2252A(a)(2), 2252(a)(2) makes it a federal criminal offense for any
4 person to knowingly receive or distribute any child pornography that has been mailed, or using any
5 means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or
6 foreign commerce by any means, including by computer.

7 INVESTIGATION

8 41. On or about December 9, 2015, NCMEC received a CyberTipline report from Twitter
9 in accordance with Title 18 U.S.C. § 2258A. Twitter reported the files bRtv8HO6.png and
10 BXZoZNUj.jpg, which contain images depicting the Sexual Exploitation of Children, were found on
11 the Twitter account belonging to the Account ID 334401627. Account ID 334401627 uploaded the
12 files bRtv8HO6.png and BXZoZNUj.jpg on or about December 7, 2015, through Twitter's photo
13 hosting service for direct messages and sent the files to Twitter Account ID 977356598.
14 Approximately 14 images of nude males were uploaded with two of the images depicting the Sexual
15 Exploitation of Children. The file bRtv8HO6.png depicts three males in a shower setting. One of the
16 males is seen performing fellatio on a minor male. The file BXZoZNUj.jpg depicts a minor male lying
17 face down on what appears to be a bed. The minor male is seen placing an object, which appears to
18 have been lubricated in his anus.

19 42. Twitter provided copies of Direct Messages from Account ID 334401627. The
20 following quotes are from the Direct Messages sent from Account ID 334401627 to Account ID
21 977356598 on or about November 30, 2015.

22 "It's hard to find boy lovers with the same interests."

23 "I hate the term Pedophile." "It sounds deranged." "Makes us sound like rapists."

24 "I prefer the term boy lover." "As it refers to the beauty and fascination of boys."

1 “Pedophiles sounds like we are rapists and out to hurt kids under 18.”

2 “I also don’t go stalking schools or playgrounds.” “Just love pics and the beauty of
3 boys.” “All we want is to love and be loved.”

4 43. On or about November 30, 2015, Account ID 977356598 asked Account ID 334401627
5 via Direct Message what was the lowest age he would go and Account ID 334401627 replied, “Prolly
6 9 or 10.”

7 44. On or about November 30, 2015, Account ID 334401627 wrote via Direct Message that
8 he never erased the message Account ID 977356598 had sent him and that he keeps the images people
9 send “for wanking, pleasure, guilt, therapy.”

10 45. On or about December 3, 2015, Account ID 334401627 wrote via Direct Message to
11 Account ID 977356598 that he was ok, “Just having internet problems.” Account ID 334401627 wrote,
12 “Using my dinosaur computer, but it takes a while to get messages to you.” Account ID 334401627
13 wrote his iPad was acting weird.

14 46. The following quotes are from Direct Messages sent from Account ID 334401627 to
15 Account ID 977356598 on or about December 7, 2015.

16 “I love the ginger boys.” “Red hair pubes turn me on.”

17 “I love my young boys.” “I can’t help who I am.”

18 “I love boys who are starting puberty with littlee pubes of hair.” “It’s my ice cream.”

19 **IDENTIFICATION OF RUSSELL ROMERO**

20 47. Twitter records reflect the account for ID 334401627 was created on 07/13/2011 and
21 updated on 12/09/2015. The email address provided was rxrromero4@q.com with the screen name
22 RXRom. The creation IP address was 75.173.81.228 and the account was created via the web.
23 Twitter’s email address history shows Account ID 334401627 email address was changed on
24 07/13/2011 to rxrromero4@q.com. Twitter records show the physical device associated with Account

1 ID 334401627 as a phone device with the phone number “+15054536156.” Virgin Mobile was listed
2 as the carrier for the account, which was created on 12/07/2015.

3 48. A search of Geo-Lookup, an internet tool used to find information regarding Internet
4 Protocol Addresses (IP address), was searched for the IP address 75.173.81.228. Geo-Lookup revealed
5 the Internet Service Provider (ISP) for 75.173.81.228 as CenturyLink. The city, region, and postal
6 code were listed as Rio Rancho, New Mexico 87124.

7 49. A search of Spokeo a people search engine that organizes White Pages listings, public
8 records, and social network information to help find and learn about people was searched for the email
9 address rxrromero4@q.com. Spokeo revealed what appears to be the user’s disabled Twitter profile
10 which had the following: the name Russell Romero, male, age 44, with his most recent address as 77
11 Sommerset Dr. SE, Rio Rancho, New Mexico 87124.

12 50. A search of Neustar iTACT, an internet tool used to identify the subscriber and carrier
13 information for telephone numbers, revealed the number 5054536156 is a telephone number for a
14 prepaid wireless phone that was active for one month or less. The carrier was listed as Sprint
15 Spectrum LP. The subscriber name was listed as Romero Russell with an address of 77 Sommerset
16 Dr. SE, Rio Rancho, NM 87124.

17 51. A search of TLO, an online investigative database for the name ‘Russell R Romero’ in
18 Rio Rancho, NM disclosed the following: Name: Russell R Romero, Date of Birth: 09/XX/1971,
19 Born 44 years, SSN: XXX-XX-3777. Possible telephone numbers associated with Russell Romero are
20 (505) 453-6156 and (505) 438-6032. Email addresses associated with Russell Romero were
21 amworld@next-wave.net, russellromero1@excite.com, russellromero@earthlink.net,
22 rromero4574@aol.com, muddystories@excite.com, and rxrromero4@hughes.net. The most recent
23 address listed for Russell Romero is 77 Sommerset Dr. SE, Rio Rancho, NM 87124.

52. A search of Facebook using 5054536156 revealed the following:
<http://www.facebook.com/rrromero>, Russell R. Romero, lives in Rio Rancho, New Mexico, from Santa Fe, New Mexico.

VERIFICATION OF TARGET AND SUBJECT PREMISES

53. On or about February 8, 2016, the United States Department of Justice Criminal Division, Child Exploitation and Obscenity Section issued as administrative subpoena to Custodian of Records, CenturyLink, for account information associated with rxrromero4@q.com and IP address 97.123.16.112 on 12/07/2015 between 04:57:10 UTC and 04:59:00 ^{UTC JRB 8/17} ~~EST~~, which is information from the Twitter database related to Twitter Account ID 334401627. On or about February 22, 2016, CenturyLink provided the following relevant information.

Start: 11/27/15 01:22:13

End: 12/12/15 04:40:34

User ID: romerorussell

Name: Romero, Russell

Email: None

TN: None; Stand-alone DSL

Service Address: Russell Romero, 77 Sommerset Dr. SE, Rio Rancho

Billing Address: Russell Romero, 77 Somerset Dr. SE, 87124 Rio Rancho NM

Length of Service: 04/19/11 to Present

54. On or about February 8, 2016, the United States Department of Justice Criminal Division, Child Exploitation and Obscenity Section issued as administrative subpoena to Subpoena Compliance, Sprint Corporation, for subscriber information from January 2013 to present for the telephone number 505-453-6156, which is information from the Twitter database related to Twitter

1 Account ID 334401627. On or about February 17, 2016, Sprint provided the following relevant
2 information.

3 Billing Account Number: 441234910

4 Account Establish Date: 11/10/2010

5 Account Expiration (cancel) date: Active through date searched.

6 Account Billing Address: Russell Romero, 77 Sommerset Dr. SE, Rio Rancho, NM
7 87124.

8 55. A check with the Division of Motor Vehicles, on or about March 8, 2016, revealed an
9 individual named Russell R. Romero with a date of birth September XX, 1971 resides at 77 Sommerset
10 Drive SE, Rio Rancho, New Mexico 87124.

11 56. On or about April 1, 2016, representatives of the U.S. Postal Service stated Russell R.
12 Romero is currently receiving mail at 77 Sommerset Drive SE, Rio Rancho, New Mexico 87124.

13 57. A search of Accurint and CLEAR information databases (public records databases that
14 provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) were
15 conducted for Russell Romero. These public records indicated that Russell R. Romero's current
16 address is 77 Sommerset Drive SE, Rio Rancho, New Mexico 87124. The records reflect Russell
17 Romero as the registered owner of a 1998 GMC Sonoma pickup truck and a 1994 Ford F150 pickup
18 truck.

19 58. Surveillance was conducted on the residence located at 77 Sommerset Drive SE, Rio
20 Rancho, New Mexico 87124 on or about March 31, 2016. No individuals or vehicles were seen at the
21 residence.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE
POSSESSION AND DISTRIBUTION OF CHILD PORNOGRAPHY**

59. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in the possession and distribution of child pornography:

60. Those who possess and distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

61. Those who possess and distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

62. Those who possess and distribute child pornography often possess and maintain their "hard copies" of child pornographic material, that is , their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

63. Those who possess and distribute child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by,

1 usually at the individual's residence, to enable the collector to view the collection, which is valued
2 highly.

3 64. Those who possess and distribute child pornography also may correspond with and/or
4 meet others to share information and materials; rarely destroy correspondence from other child
5 pornography distributors/collectors; conceal such correspondence as they do their sexually explicit
6 material; and often maintain lists of names, addresses, and telephone numbers of individuals with
7 whom they have been in contact and who share the same interests in child pornography.

8 65. Those who possess and distribute child pornography prefer not to be without their child
9 pornography for any prolonged time period. This behavior has been documented by law enforcement
10 officers involved in the investigation of child pornography throughout the world.

11 66. Based on the distribution of child pornography via Twitter by Russell Romero. I
12 believe Russell Romero likely displays characteristics common to individuals involved in the
13 possession and distribution of child pornography.

14 **BACKGROUND ON COMPUTERS, DIGITAL CAMERAS, AND CHILD PORNOGRAPHY**

15 67. Computers basically serve four functions in connection with Child Sexual Exploitation:
16 production, communication, distribution, and storage.

17 68. Individuals involved in the Sexual Exploitation of Children can now transfer printed
18 photographs into a computer-readable format with a device known as a scanner. Furthermore, with the
19 advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly
20 transferred to a computer by simply connecting the camera to the computer. In the last ten years, the
21 resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken
22 with digital cameras have become sharper and crisper. These memory cards often can provide enough
23 space to store thousands of high-resolution photographs. Video camcorders, which once recorded
24

1 video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in
2 the camera. The video files can be easily transferred from the camcorder to a computer.

3 69. A device known as a modem allows any computer to connect to another computer
4 through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally
5 millions of computers around the world. The ability to produce images containing the Sexual
6 Exploitation of Children easily, reproduce it inexpensively, and market it anonymously (through
7 electronic communications) has drastically changed the method of distribution and receipt of child
8 pornography. Images depicting the Sexual Exploitation of Children can be transferred via electronic
9 mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem.
10 Because of the proliferation of commercial services that provide electronic mail service, chat services
11 (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of
12 distribution and receipt of Child Sexual Exploitative material.

13 70. The computer's ability to store images in digital form makes the computer itself an ideal
14 repository for child pornography. The size of the electronic storage media (commonly referred to as
15 the hard drive) used in home computers has grown tremendously within the last several years. These
16 drives can store thousands of images at very high resolution. In addition, there are numerous options
17 available for the storage of computer or digital files. Two Terabyte external and internal hard drives
18 are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash"
19 drives, which are very small devices which are plugged into a port on the computer. It is extremely
20 easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then
21 copy it (or any other files on the computer) to any one of those media storage devices. (CDs and
22 DVDs are unique in that special software must be used or save or "burn" files onto them).

1 71. The Internet affords individuals several different venues for obtaining, viewing, and
2 trading images depicting the Sexual Exploitation of Children in a relatively secure and anonymous
3 fashion.

4 72. Individuals also use online resources to retrieve and store material containing the Sexual
5 Exploitation of Children, including services offered by Internet portals such as Yahoo! and Hotmail,
6 among others. The online services allow a user to set up an account with a remote computing service
7 that provides e-mail services as well as electronic storage of computer files in any variety of formats.
8 A user can set up an online storage account from any computer with access to the Internet. Even in
9 cases where online storage is used, however, evidence of the Sexual Exploitation of Children can be
10 found on the user's computer or external media in most cases.

11 73. As in the case with most digital technology, communications by way of computer can
12 be saved or stored on the computer used for these purposes. Storing this information can be
13 intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite
14 websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally,
15 e.g., traces of the path of an electronic communication may be automatically stored in many places
16 (e.g., temporary files or ISP client software, among others). In addition to electronic communications,
17 a computer user's Internet activities generally leave traces or "footprints" in the web cache and history
18 files of the browser used. A forensic examiner often can recover evidence suggesting whether a
19 computer contains peer to peer software, when the computer was sharing files, and some of the files
20 which were uploaded or downloaded. When a DVD or CD is played in the optical disc drive of a
21 computer, evidence regarding this activity often can be recovered from the computer's media player
22 software, Windows Registry, and recent "link" files. Such information is often maintained indefinitely
23 until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND OTHER MEDIA

74. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variant of systems and storage devices including hard disk drives, solid state drives (SSDs), floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

1 The volume of data stored on many computer systems and storage devices will
2 typically be so large that it will be highly impractical to search for data during the
3 execution of the physical search of the premises. A single gigabyte of storage space is
4 the equivalent of 500 double-spaced pages of text. A single terabyte of storage space is
5 1,000 gigabytes. Storage devices capable of storing two terabytes (TB) of data are now
6 commonplace in desktop computers.

7 Computer users can attempt to conceal data within computer equipment and
8 storage devices through a number of methods, including the use of innocuous or
9 misleading filenames and extensions. For example, files with the extension “.jpg” often
10 are image files; however, a user can easily change the extension to “.txt” to conceal the
11 image and make it appear that the file contains text. Computer users can also attempt to
12 conceal data by using encryption, which means that a password or device, such as a
13 “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition,
14 computer users can conceal data within another seemingly unrelated and innocuous file
15 in a process called “steganography.” For example, by using steganography a computer
16 user can conceal text in an image file which cannot be viewed when the image file is
17 opened. Therefore, a substantial amount of time is necessary to extract and sort through
18 data that is concealed or encrypted to determine whether it is evidence, contraband or
19 instrumentalities of a crime.

20 75. Based on my own experience and my consultation with other agents who have been
21 involved in computer searches, searching computerized information for evidence or instrumentalities
22 of a crime often requires the seizure of all of a computer system’s input and output peripheral devices,
23 related software, documentation, and data security devices (including passwords) so that a qualified
24

1 computer expert can accurately retrieve the system's data in a laboratory or other controlled
2 environment. There are several reasons that compel this conclusion:

3 The peripheral devices that allow users to enter or retrieve data from the storage
4 devices vary widely in their compatibility with other hardware and software. Many
5 system storage devices require particular input/output devices in order to read the data
6 on the system as it now operates in order to accurately retrieve the evidence listed
7 above. In addition, the analyst needs the relevant system software (operating systems,
8 interfaces, and hardware drivers) and any applications software which may have been
9 used to create the data (whether stored on hard drives or on external media), as well as
10 all related instruction manuals or other documentation and data security devices; and

11 In order to fully retrieve data from a computer system, the analyst also needs all
12 storage devices, as well as the central processing unit (CPU). In cases like the instant
13 one where the evidence consists partly of image files, the monitor and printer are also
14 essential to show the nature and quality of the graphic images which the system could
15 produce. Further, the analyst again needs all the system software (operating systems or
16 interfaces, and hardware drivers) and any applications software which may have been
17 used to create the data (whether stored on hard drives or on external media) for proper
18 data retrieval.

19 **CHARACTERISTICS OF A CHILD PORNOGRAPHY COLLECTOR**

20 76. Your affiant has reviewed and also has been informed of the studies of child sex
21 offenders in general, and child pornography offenders in particular. Your affiant has also learned
22 about the activities and characteristics of child pornography offenders from other law enforcement
23 agents and officers with who focus on online child sexual exploitation, including those who investigate
24 the offenses and those who analyze the computer equipment of these offenders.

1 77. Based on what I have learned from other individuals who specialize in the investigation
2 and study of child pornography offenders, I know that the following traits and characteristics are
3 generally found to exist and be true in cases involving individuals who collect images depicting the
4 Sexual Exploitation of Children:

5 a. The majority of individuals who collect images depicting the Sexual
6 Exploitation of Children are persons who have a sexual attraction to children. They
7 receive sexual gratification and satisfaction from sexual fantasies fueled by depictions
8 of children that are sexual in nature.

9 b. The majority of individuals who collect images depicting the Sexual
10 Exploitation of Children also collect sexually explicit materials, which may consist of
11 photographs, magazines, motion pictures, videotapes, books, slides, computer graphics
12 or digital or images for their own sexual gratification. The majority of these individuals
13 also collect child erotica, which may consist of images or text that do not rise to the
14 level of child pornography but which nonetheless fuel their deviant sexual fantasies
15 involving children.

16 c. The majority of individuals who collect images depicting the Sexual
17 Exploitation of Children often seek out like-minded individuals, either in person or on
18 the Internet, to share information and trade depictions of child pornography and child
19 erotica as a means of gaining status, trust, acceptance and support. This contact also
20 helps these individuals to rationalize and validate their deviant sexual interest and
21 associated behavior. The different Internet-based vehicles used by such individuals to
22 communicate with each other include, but are not limited to P2P, email groups, bulletin
23 boards, newsgroups, instant messaging and other similar devices.
24

1 d. The majority of individuals who collect images depicting the Sexual
2 Exploitation of Children possess and maintain books, magazines, newspapers and other
3 writings, in hard copy or digital medium, on the subject of sexual activities of children
4 as a way of understanding their own feelings toward children, justifying those feelings
5 and finding comfort for their illicit behavior and desires. Such individuals rarely
6 destroy these materials because of the psychological support they provide.

7 e. The majority of individuals who collect images depicting the Sexual
8 Exploitation of Children often collect, read, copy or maintain names addresses
9 (including email addresses, phone numbers, or lists of persons who have advertised
10 otherwise made known in publications and on the Internet that they have similar
11 interests. These contacts are maintained as a means of personal referral, exchange or
12 commercial profit. These names may be maintained in the original medium from which
13 they were derived, in telephone books or notebooks, on computer storage devices or
14 merely on scraps of paper.

15 f. The majority of individuals who collect images depicting the Sexual
16 Exploitation of Children rarely, if ever, dispose of their sexually explicit materials and
17 may go to great lengths to conceal and protect from discovery, theft, and damage to
18 their collections of illicit materials.

19 78. Based on the experience of other law enforcement agents who specialize in
20 investigating computer-facilitated child sexual exploitation crimes and with whom I have consulted, I
21 believe that the majority of individuals who collect images depicting the Sexual Exploitation of
22 Children and/or child pornography via the Internet maintain their collections, increasingly in both
23 online and offline storage media, even as they relocate from one residential or work address to another.
24

CONCLUSION

79. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. § 2252(a)(1), 18 U.S.C. § 2252A(a)(1) and 18 U.S.C. § 2252(a)(4)(B), 18 U.S.C. § 2252A(a)(5)(B), and 18 U.S.C. § 2252(a)(2), 18 U.S.C. § 2252A(a)(2) .

80. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,


RHONDA BOWIE
U.S. Postal Inspector

Subscribed and Sworn to before me this 3rd day of May, 2016.


UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The premises to be searched is located at 77 Sommerset Drive SE, Rio Rancho, New Mexico 87124, including the surrounding grounds, any garages, sheds, storage rooms, storage lockers, trash containers, any outbuildings located thereon. The premises being more particularly described as a one story single family home. The house is tan in color with brick on the lower half of the home. The house has dark brown trim with dark brown railing in front of the porch. The numbers "77" are clearly displayed on the front of the house under the porch light.

ATTACHMENT B**ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252(a)(1), 18 U.S.C. § 2252A(a)(1) and 18 U.S.C. § 2252(a)(4)(B), 18 U.S.C. § 2252A(a)(5)(B), and 18 U.S.C. § 2252(a)(2), 18 U.S.C. § 2252A(a)(2):

1. Computer(s), computer hardware, computer software, computer-related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, digital video disc (DVD) players, video display monitors, cell phones, flash drives, external hard drives or any other electronic media or digital media storage devices, that may be, or are used to : visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. All originals, copies, and negatives of images depicting the Sexual Exploitation of Children as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and child erotica, in any format or medium (including, but not limited to, computer or digital data files, photographs, magazines photocopies, DVDs, compact discs (CDs), VHS tapes, videotapes, and photographic and motion picture film).

3. All visual depictions of minors.

4. All DVDs, CDs, VHS tapes, and videotapes.

5. All cameras, film, and other photographic equipment.

6. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters,

1 papers, handwritten notes, and electronic messages, chat logs and electronic records) pertaining to the
2 possession, receipt, distribution, transportation, or sale of images depicting the Sexual Exploitation of
3 Children as defined in 18 U.S.C. § 2256(8), or to the possession, receipt, distribution, transportation, or
4 sale of visual depictions of Minors engaged in Sexually Explicit Conduct as defined in 18 U.S.C. §
5 2256(2).

6 7. All notes, documents, records, correspondence, diaries, and address books, in any
7 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
8 papers, handwritten notes, and electronic messages, chat logs and electronic records) identifying
9 individuals or companies distributing, transporting, selling, or receiving images depicting the Sexual
10 Exploitation of Children as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in
11 sexually explicit conduct as defined in 18 U.S.C. § 2256(2), through interstate or foreign commerce by
12 any means including, but not limited to, by United States mail or computer).

13 8. All notes, documents, records, correspondence, diaries, and address books, in any
14 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
15 papers, handwritten notes, and electronic messages, chat logs and electronic records), identifying
16 individuals or companies possessing images depicting the Sexual Exploitation of Children as defined
17 in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined
18 in 18 U.S.C. § 2256(2).

19 9. All notes, documents, records, correspondence, diaries, and address books, in any
20 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
21 papers, handwritten notes, and electronic messages, chat logs and electronic records), concerning
22 communications between individuals or companies about images depicting the Sexual Exploitation of
23 Children as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit
24 conduct as defined in 18 U.S.C. § 2256(2).

1 10. All notes, documents, records, correspondence, diaries, and address books, in any
2 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
3 papers, handwritten notes, and electronic messages, chat logs and electronic records) concerning
4 subscriptions to or memberships in groups, clubs, or services that provide or make images depicting
5 the Sexual Exploitation of Children as defined in 18 U.S.C. § 2256(8), or visual depictions of minors
6 engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), accessible to subscribers or
7 members.

8 11. All notes, documents, records, correspondence, diaries, and address books, in any
9 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
10 papers, handwritten notes, and electronic messages, chat logs and electronic records) identifying
11 individuals or companies that may have contacted Russell Romero or have been contacted by Russell
12 Romero, by any means for the purpose of receiving, distributing, transporting, or selling images
13 depicting the Sexual Exploitation of Children as defined in 18 U.S.C. § 2256(8) or visual depictions of
14 minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

15 12. All notes, documents, records, correspondence, diaries, and address books, in any
16 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
17 papers, handwritten notes, and electronic messages, chat logs and electronic records) identifying
18 individuals that may have contacted Russell Romero or have been contacted by Russell Romero, via
19 Twitter, tweets, direct messages, or any means for the purpose of receiving, distributing, transporting,
20 or selling images depicting the Sexual Exploitation of Children as defined in 18 U.S.C. § 2256(8) or
21 visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

22 13. All notes, documents, records, correspondence, diaries, and address books, in any
23 format or medium (including, but not limited to, computer or digital data files, mailing lists, supplier
24 lists, mailing address labels, envelopes, letters, papers, handwritten notes, and electronic messages,

1 chat logs and electronic records) pertaining to the preparation, purchase, or acquisition of names of
2 individuals or companies, or lists of names of individuals or companies, to be used in connection with
3 the receipt, distribution, transportation, or sale of images depicting the Sexual Exploitation of Children
4 as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct
5 as defined in 18 U.S.C. § 2256(2), through interstate or foreign commerce by any means (including,
6 but not limited to, by United States mail or computer).

7 14. All notes, documents, records, correspondence, diaries, and address books, in any
8 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
9 papers, handwritten notes, and electronic messages, chat logs and electronic records) reflecting a
10 sexual interest in minors, or personal contact or activities with minors.

11 15. All notes, documents, records, correspondence, diaries, and address books, in any
12 format or medium (including, but not limited to, computer or digital data files, envelopes, letters,
13 papers, handwritten notes, and electronic messages, chat logs and electronic records) containing or
14 listing names and addresses of minors who are visually depicted while engaged in sexually explicit
15 conduct, as defined by 18 U.S.C. § 2256.

16 16. All notes, documents, records, correspondence, diaries, and address books, in any
17 format or medium (including, but not limited to, computer or digital data files, invoices, billing
18 statements, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and
19 electronic records) that concern any accounts with an Internet Service Provider.

20 17. All notes, documents, records, correspondence, diaries, and address books, in any
21 format or medium (including, but not limited to, computer or digital data files, invoices, billing
22 statements, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and
23 electronic records), that concern online storage or other remote computer storage, including, but not
24 limited to, software used to access such online storage or remote computer storage, user logs or

1 archived data that show connection to such online storage or remote computer storage, and user logins
2 and passwords for such online storage or remote computer storage.

3 18. All notes, documents, records, correspondence, diaries, and address books, in any
4 format or medium (including, but not limited to, computer or digital data files, invoices, billing
5 statements, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and
6 electronic records) that evidence ownership, use, or control of any computer(s) and all related
7 computer and/or video equipment found in the premises listed and described in Attachment A.

8 19. All notes, documents, records, correspondence, diaries, and address books, in any
9 format or medium (including, but not limited to, computer or digital data files, envelopes, rental or
10 lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, addressed
11 correspondence, letters, papers, handwritten notes, and electronic messages, chat logs and electronic
12 records) pertaining to occupancy or ownership of the premises listed and described in Attachment A.

13 20. For any computer hard drive or other electronic media found to contain information
14 otherwise called for by this warrant:

- 15 a. Evidence of who used, owned or controlled the computer at the time the things
16 described in this warrant were created, edited, or deleted, such as logs, registry
17 entries, saved usernames and passwords, documents, and browsing history;
- 18 b. Evidence of software that would allow others to control the computer, such as
19 viruses, Trojan horses, and other forms of malicious software;
- 20 c. Evidence of the attachment to the computer of other storage devices, disks, CD-
21 ROMs, or similar containers for electronic evidence;
- 22 d. Evidence of the times the computer was used;
- 23 e. Passwords, encryption keys, and other access devices that may be necessary to
24 access the computer.

1 f. Documentation and manuals that may be necessary to access or conduct an
2 examination of the computer.

3 ~~21. Any and all guns and firearms.~~ *SCY*

4 22. Any and all records of indicia of occupancy, residency, or ownership of the premises or
5 motorized conveyances, such as leases, utility bills, registration, and cancelled mail.